Identity Theft Assistance Guide

As your local community bank, Midwest Bank of Western Illinois works diligently to protect our customer's personal information and safety. One of our goals is to educate our customers about Identity Theft, the steps you can take to protect yourself and your personal and account information. You can use this resource tool to take action in case you suspect that your account has been compromised or you have been a victim of identity theft.

Important Contact Information

Monmouth Police Department	(309) 734-8383	
Warren County Sheriff	(309) 734-8505	
Social Security Fraud Hotline	(800) 269-0271	www.socialsecurity.gov
United States Postal Service	(800) 275-8777	www.usps.com
Federal Trade Commission ID Theft Hotline	(877) 438-4338	www.consumer.gov/idtheft
Securities & Exchange Commission	(800) 732-0330	www.sec.gov
Telecheck	(800) 710-9898	
Federal Bureau of Investigations		www.fbi.gov
U.S. Secret Service		www.treas.gov/usss

Credit Bureaus

• Equifax	(888) 766-0008	www.equifax.com
• Experian	(888) 397-3742	www.experian.com
• TransUnion	(800) 680-7289	www.transunion.com

Customer Educational Tools

- Stay Safe Online — www.staysafeonline.org
- OnGuard Online — www.onguardonline.gov

How Identity Theft Happens

Identity theft is a serious crime. People whose identities have been stolen can spend months or years cleaning up the mess the thieves have made of a victims good name and credit record.

Approximately 15 million US consumers have their identities stolen and used fraudulently each year with financial losses totaling upwards of $50 billion. Close to 100 million additional Americans have their personal identifying information placed at risk of identity theft each year when records maintained in government and corporate databases are lost and stolen.*

As the methods used to perform identity theft continue to grow, so do the types of accounts and services being stolen by these criminals. You can be extremely careful about protecting your personal information, but despite your best efforts, skilled thieves have a variety of methods to get your data and use it for their own benefit.

Here are the most common ways:

- "Phishing". You get an email that appears to be from your bank, credit card or Investment Company, online service such as PayPal or eBay etc., instructing you to click on a link and provide information to verify your account.

- "Vishing" (voice Phishing). You get an automated phone message asking you to call your bank of credit card company (typically for an urgent matter or problem with your account). Even your caller ID is fooled. You call the number provided on the message and are asked to enter in your account number, debit card number and PIN, or other personal information.

- Malware (Short for Malicious Software). You unknowingly downloaded malicious software when you have opened an attachment, clicked on a pop-up box or downloaded a song or a game. Criminals can use spyware to record your keystrokes, obtain credit card numbers, bank account information and passwords. Thieves can also access confidential information on your computers' hard drive.

- "Pharming" or spoofing. Computer hackers can redirect a legitimate Web site's traffic to an imposter site where you will be asked to provide confidential personal information.

- "Smishing". This is phishing done with text messaging on your cell phone.

*information obtained from public documentation and websites

- ATM skimming. Thieves steal your credit/debit card numbers and PINs by capturing the information in a data storage device. They may swipe your card for an actual purchase, or attach a device to an ATM machine where you enter or swipe your card.

- Thieves may steal your mail; including bank and credit card statements, re-issued credit and debit cards, new checks and tax information. Thieves may also complete and return credit card solicitations sent out in the mail.

- They may rummage through your trash; the trash of businesses or public dumpsters in a practice known as "dumpster diving."

- Thieves may steal your wallet, purse or burglarize your home stealing personal information they find in your home.

How Thieves Use Your Personal Information

As soon as a thief has your personal information, there are many methods available for them to scam you and use your information without your knowledge. They can:

- Forge checks or create bogus debit cards and drain your bank account.
- Open a new bank account in your name, enabling them to write bad checks. Thieves can also apply for credit card accounts, usually maxing out the credit line on the account. Because your bills are being sent to a different address, it may be quite some time before you realize there is a problem.

- Obtain identification such as a driver's license issued with their picture, utilizing your personal information.

- Purchase a car or luxury item by taking out a loan in your name with your identification.

- Establish cell phone or wireless service in your name.

- All these delinquent accounts are reported on your credit report, ruining your credit score, preventing you from obtaining legitimate financing, opening new accounts, purchasing vehicles, obtaining a mortgage or ruining your chance at employment.

Tips to Help Prevent Identity Theft

A main priority for Midwest Bank of Western Illinois is to protect your personal information and keep your account information safe. Here are some tips that you can do to help in keeping your information safe:

- Carry only the items that you need in your purse/wallet. The less personal information that you have on you, the better off you will be if your purse or wallet is

stolen. Never carry your Social Security Card; leave it in a secure place and memorize the number.

- Report lost or stolen credit and debit cards immediately – call each credit card issuer and ask to have the stolen card accounts closed and new ones opened to replace them.

- Cancel any credit card accounts that you no longer use – destroy these cards with a cross-cut shredder.

- Report lost or stolen checks immediately. If you bank with Midwest Bank, we will block payment on the stolen items. Make sure that you review your checking account statements and verify that the checks that have posted to your account were written by you. We recommend that you sign up for our Internet Banking so that you can monitor your accounts, balances and checks/debits that are posting to your account. This is one of the most valuable tools available to you, free of charge.

- We recommend that you do not include the following personal information on your checks; driver's license, telephone or Social Security numbers.

- Don't put outgoing mail in or on your mailbox. Thieves may use your mail to steal your identity.

- Discard mail appropriately. Thieves may pick through your trash to try and retrieve documents containing your personal information or credit card offers you get in the mail. To avoid these issues, purchase a cross-cut shredder and destroy the documents accordingly.

- Guard your Personal Identification Numbers (PINs). Memorize your information; do not write your PIN on your Debit/ATM or credit cards and don't keep your PINs with your cards. Be careful with ATM and credit card receipts as thieves can use them to access your accounts. Never throwaway receipts in a public trash can, shred them instead.

- Keep track of your regular monthly bills and statements sent out in the mail. If a bill fails to reach you, call the company to find out why you haven't received it. Someone may have filed a false "change of address" notice to redirect the statement to a different address. Contact the company to investigate if they offer electronic statements that you can receive in your secure Internet Banking environment. Studies have shown that you are 40% less likely to be a victim of identity theft when switching to paperless billing.

- Protect your identity while online; when conducting financial transactions or making purchases on the web, make sure the websites you are visiting are secure and protect your data. Look for websites that use Secure Socket Layer (SSL) technology to

encrypt your personal information. You can also check to see if your session is secure by looking for a small lock symbol located in the lower corner of your browser window. You may also look for the letters https:// at the beginning of the website URL in your browser. The "s" means that the web connection is secure.

- Review your credit report annually-you can check your credit report from each of the three major credit reporting agencies for free, once a year. Go to www.annualcreditreport.com. Review the report - if you notice any credit cards and loans that do not belong to you, contact the companies and credit reporting agencies immediately.

Recovering from Fraud – Key Steps to Take if You Are a Victim of Identity Theft or Fraud

If you are a victim of identity theft or fraud, take the following steps as soon as possible. Keep a log of all related phone conversations, including the names of people with whom you spoke with and copies of all correspondence. Key steps to restore your identity:

1. **Review your credit reports and place a fraud alert on your credit reports.** Placing a fraud alert can help prevent a thief from opening any more accounts in your name. Contact one of the toll-free fraud numbers of any of the three consumer reporting companies to place the alert on your credit report. The company you call is required to contact the other two, which will place an alert on their report as well.

   Equifax: (888) 766-0008
   Equifax Fraud Assistance
   PO Box 740241
   Atlanta, GA 30374-0241
   www.equifax.com

   Experian: (888) 397-3742
   Experian Fraud Assistance
   PO Box 9532
   Allen, TX 75013
   www.experian.com

   TransUnion: (800) 680-7289
   Fraud Victim Assistance Division
   PO Box 6790
   Fullerton, CA 92834-6790
   www.transunion.com

   Place a block or freeze on your credit bureau and send a letter to the credit bureau and credit companies. Sample letters are included in this guide.

2. **Report the fraud to the authorities**
   It is recommended that you contact your local law enforcement agencies to file a report regarding the fraudulent activity. Contact government agencies such as the Federal Trade Commission (FTC) to report the fraudulent activity. The FTC will put your information into a secure consumer fraud database and may, in appropriate instances, share it with other law enforcement agencies.

   Contact companies with whom you have relationships with and speak with someone in the security or fraud department. Inform them that your accounts may be compromised or that you have been a victim of identity theft. Banks and card companies may issue new cards and PINs to protect your assets, and will work to identify and rectify any unauthorized charges.

   Notify your financial institution to stop checks or report stolen checks. If there are fraudulent debits on your account, request forms to dispute the transactions and close out accounts accordingly. Contact any companies on your credit report that you do not recognize. Verify the information they have in their records for the reported item. Provide the creditor with a copy of your police report, notarized FTC Affidavit or other relevant documentation.

3. **Follow up is key**
   Follow up with companies and agencies that you have contacted to ensure that their investigation has resulted in your favor. Even though you may be the victim, you have certain responsibilities. By working with credit grantors to identify all fraudulent accounts, you can greatly reduce this crime's effects on you.

4. **Are there laws that protect me from fraud and identity theft?**
   Your Rights-The federal Fair Credit Reporting Act (FCRA) is designed to promote accuracy, fairness and privacy of information in the files of every "consumer reporting agency" (CRA). Most CRAs are credit bureaus that gather and sell information about you — such as, if you pay your bills on time or have filed bankruptcy, to creditors, employers, landlords and other businesses with a permissible purpose. You can find the complete text of the FCRA, 15 U.S.C. 1681-1681u, at the Federal Trade Commission's Web site. As a consumer, you have specific FCRA rights. You may have additional rights under state law and can contact a state or local consumer protection agency or a state attorney general to learn those rights

Sample Letter- Blocking/Freezing information at Credit Bureau

Date

Complaint/Fraud Department
Name of Credit Bureau
Address
City, State and Zip code

Your Name
Your Address
Your City, State and Zip code
Your Social Security Number

Dear Sir or Madam:

I am a victim of Identity Theft/Fraud. I am writing to request that you block the following fraudulent information in my file. This information does not relate to any transaction that I have made. I have circled the fraudulent items on the attached copy of my credit bureau/statement.

Enclosed is a copy of the law enforcement report regarding my Identity Theft or Fraud. Please let me know if you need any additional information from me to block/freeze this information on my credit report.

Sincerely,

Your Name

Enclosures:

Sample Dispute Letter-Existing Accounts

Date

Name of Creditor
Attn: Fraud Department
Address
City, State and Zip code

Your Name
Your Address
City, State and Zip code
Social Security Number
Account Number

Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) on my account in the amount of $_____. I am a victim of identity theft and I did not make this (charge or debit). I am requesting that the (charge/debit be removed), that any finance and other charges related to the fraudulent amount be credited back to me. Please forward a copy of the accurate statement reflecting these changes.

Enclosed are copies of documentation supporting my case. Please investigate this matter and correct the fraudulent charge/debit as soon as possible.

Sincerely,

Your Name

Enclosures:

Charting Your Steps

Use this form to record the steps you have taken to report the fraudulent use of your identity. Keep this list in a safe place for your reference.

Credit Bureaus

Credit Bureau	Phone Number	Date Contacted	Contact Person	Comments
Equifax	(888) 766-0008			
Experian	(888) 397-3742			
TransUnion	(800) 680-7289			

Banks, Credit Card Issuers and other Creditors

Creditor	Address/ Phone #	Date Contacted	Contact Person	Comments

Law Enforcement Agencies

Agency	Phone Number	Date Contacted	Contact Person	Comments
Monmouth Police	**309- 734-8383**			
Warren Co Sheriff	**309- 734-8505**			
FTC	**877- 438-4338**			

Educational Resources to assist in Internet Security, Identity Theft, and Phishing

Stay Safe Online
http://www.staysafeonline.org/

OnGuard Online
http://www.onguardonline.gov/

MS-ISAC Newsletter – Security and Privacy on Social Networking Sites
http://msisac.cisecurity.org/newsletters/2010-03.cfm

MS-ISAC Daily Tip – Stay Safe on Social Networking Sites
http://msisac.cisecurity.org/daily-tips/Stay-Safe-on-Social-Networking-Sites.cfm

US-CERT Cyber Security Tip – Staying Safe on Social Networking Sites
http://www.us-cert.gov/cas/tips/ST06-003.HTML

National Cyber Security Alliance – Protect Yourself: Social Networking
http://staysafeonline.org/in-the-home/social-networking

Facebook Security Guide (issued in October 2011)
https://www.facebook.com/safety/attachment/Guide%20to%20Facebook%20Security.pdf

Cyber Security Newsletter Tips
http://www.msisac.org/awareness/news/?

How do I protect the information on my smartphone?

We have come to depend on our smartphones so heavily that it is hard to remember what we did before we had them. If you have a smartphone, you now carry a fully functional computer in your pocket or purse. That is a tremendous amount of information at your fingertips! Therefore, it is paramount that you safeguard the smartphone.

Common Risks for Smartphones
Take a moment to consider each of these areas:

- **Loss of device and information theft.** Smartphones are small and can easily be lost or stolen. Unauthorized users may access your accounts, address lists, photos, and more to scam, harm, or embarrass you or your friends. They may leverage stored passwords to access your bank and credit card accounts, steal your money, or make credit card charges. They may also gain access to sensitive material.

- **Social engineering.** A common mobile threat is social engineering. Whether via text message, image, or application (app) to download, an incoming communication may be an attempt to gain access to your information. A current example consists of a text message that comes from an unknown number telling you that if you click on the link provided, you will have access to thousands of free ringtones. If this sounds too good to be true, that is because it is. The link is a malicious link. Clicking on it will compromise the security of your smartphone.

- **TMI (too much information).** Guidelines for protecting privacy, safety, and reputation when sharing via computers also apply when sharing via smartphones. Mobile devices enable instantaneous capturing, posting, and distribution of images, videos, and information. They may also broadcast location information.

- **Public Wi-Fi.** Smartphones are susceptible to malware and hacking when leveraging unsecured public networks.

- **Bluetooth® and near field communications (NFC).** Bluetooth is a wireless network technology that uses short-wave radio transmissions to transmit voice and data. NFC allows for smartphones to communicate with each other by simply touching another smartphone, or being in close proximity to another smartphone with NFC capabilities or an NFC device. Risks with using NFC and Bluetooth include eavesdropping, through which the cybercriminal can intercept data transmission, such as credit card numbers. NFC also has the risk of transferring viruses or other malware from one NFC-enabled device to another.

Simple Steps to Protect Your Smartphone

- **Update the operating system.** Smartphones are computing devices that need to be updated. Updates often provide you with enhanced functionality and enriched

features, as well as fixes to critical security vulnerabilities. Your smartphone manufacturer should notify you whenever an update is available.

- **Use of security software is a must.** As the smartphone market is increasing, so too is the amount of malware designed to attack smartphones. The software security solutions that are available for desktops and laptops are not as widely available for smartphones. A key protection is to use mobile security software and keep it up to date. Many of these programs can also locate a missing or stolen smartphone, back up your data, and even remotely wipe all data from the smartphone if it is reported stolen.

- **Password-protect your device.** Enable strong password protection on your device and include a timeout that requires authentication after a period of inactivity. Secure the smartphone with a unique password – not the default one it came with. Do not share your password with others.

- **Think before you click, download, forward, or open.** Before responding, registering, downloading, or providing information, get the facts. No matter how tempting the text, image, or application is, if the download is not from a legitimate app store or the site of a trusted company, do not engage with the message.

- **Understand the terms of use.** Some applications claim extensive rights to accessing and leveraging your personal information. If the app requires more access to your account or device than is needed to run the service, do not continue. In addition, be aware that terms can change over time. Review your terms of use often.

- **Be cautious with public Wi-Fi.** Many smartphone users use free Wi-Fi hotspots to access data and keep their smartphone plan costs down. There are numerous threats associated with Wi-Fi hotspots. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.

- **Disable Bluetooth and NFC capabilities when not in use.** Capabilities such as Bluetooth and NFC can provide ease and convenience in using your smartphone. They can also provide an easy way for a nearby, unauthorized user to gain access to your data. Turn these features off when they are not required.

- **Enable encryption.** Enabling encryption on your smartphone is one of the best ways to safeguard information stored on the device, thwarting unauthorized access.

- **Securely dispose of your device.** With the constant changes and upgrades in the smartphone market, many are upgrading their devices on a regular basis. It is important that you wipe the information from your smartphone before disposal. Additionally, make sure any secure digital (SD) cards are removed and erased. If you are not redeploying the subscriber identity module (SIM) card to another device, then make sure your personal information stored on the SIM card is erased or destroyed.

For additional information, please visit the following sites:

- **About.com – 14 Ways to Find a Stolen or Lost iPhone:** http://ipod.about.com/od/iphonetroubleshooting/tp/14-Ways-To-Find-A-Lost-Or-Stolen-Iphone.htm
- **FTC – How to Dispose Your Mobile Device Securely:** http://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device
- **US-CERT – Cyber Threats to Mobile Phones:** http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf
- **Sophos – Android Tool:** http://www.sophos.com/androidsecurity

Microsoft – Secure Your Smartphone: http://www.microsoft.com/security/online-privacy/mobile-phone-safety.aspx